



REQUEST FOR PROPOSALS

ISSUE DATE: August 15, 2025

DUE DATE: September 12, 2025

TIME: 10:00 a.m.

If further information is required, please send an email to : bids@utaw.org

United Talmudical Academy (UTAW) is issuing this Request for Proposals (RFP #85-018) in respect of the following items that together will comprise the components of its **Cybersecurity 85 Pilot Program**. Qualified prospective bidders may bid on any one or more of the items listed herebelow.

UTAW is a private school network with 13 campuses around the Williamsburg area of Brooklyn, NY. The deliverables listed herein are to be implemented at its main data center location, also in the same geographical vicinity.

Bids must include a proposal for implementation and a firm inclusive quotation for the item(s) being bid for that includes any capital costs, services for installations (together the CapEx component of the proposal) and recurring operational costs (such as subscriptions, support etc.) for a duration of 3 years (the OpEx component of the proposal). The in-scope station or user count for this **Cybersecurity 85 Pilot Program** is to be assumed to number 1,000.

All bids must be submitted by Electronic Mail to: bids@utaw.org no later than 10am on September 15, 2025.

The following pages list the deliverables to be bid on; these are divided into named categories. Bidders may bid on any or all of the categories or any components thereof. Please indicate in the cover of your bid, which deliverables you are bidding on.

REMAINDER OF THIS PAGE IS LEFT INTENTIONALLY BLANK

Categories:

1) Perimeter Update

UTAW requires proposals in respect of updating its **Advanced/Next-Generation Firewalls** stance and infrastructure. The proposal can be based either on the provisioning of Firewalls that will be owned and operated solely by UTAW (CapEx+OpEx Model), or as “Firewall as a Service” (FWaaS) offering whereby the combined costs of provisioning and maintaining the Firewalls will be invoiced as recurring operational expenses (“OpEx”) to UTAW.

The solution being proposed for this category must include or consider the following functions:

- Advanced Threat Detection and Prevention
- AI/ML Threat Detection and Response
- Application Awareness & Control
- Cloud-Delivered Threat Intelligence
- Secure Sockets Layer (SSL) inspections
- Deep Packet Inspection (DPI)
- Intrusion prevention/detection
- Malware Detection
- Integrated Intrusion Prevention Systems (IIPS)
- Virtual Private Network (VPN)
- Content blocking and filtering/uniform resource locator (URL) filtering
- Domain Name System (DNS)/DNS-layer security, blocking, and filtering
- Intrusion Detection Systems (IDS)
- Secure Access Service Edge (SASE)
- Zero Trust Architecture (ZTNA)

The solution may be proposed as either a single product/offering or a combination of offerings that together offer the functionality that is required.

REMAINDER OF THIS PAGE IS LEFT INTENTIONALLY BLANK

2) Functional Traffic Separation

UTAW requires proposals in respect of updating its network infrastructure to provide advanced **Network Segmentation**, including both N/S and E/W segmentation.

The proposal can be based either on the provisioning of a Hardware, Software or a Converged solution that will be owned and operated solely by UTAW (CapEx+OpEx Model), or as “Network Segmentation as a Service” (NSaaS) offering whereby the combined costs of provisioning and maintaining the solution will be invoiced as a recurring operational expense (“OpEx”) to UTAW.

3) Enhanced System Resilience

UTAW requires proposals in respect of updating its **Endpoint Protection** stance and infrastructure. The proposal can be based either on the provisioning of a solution that will be owned and operated solely by UTAW (CapEx+OpEx Model), or as a subscription based offering whereby the combined costs of provisioning and maintaining the solution will be invoiced as recurring operational expenses (“OpEx”) to UTAW. It can also be proposed as a hybrid of these two models.

The solution being proposed for this category must include of consider the following functions:

- Anti-malware
- Anti-ransomware
- Anti-spam
- Anti-virus
- Endpoint Detection & Response (EDR)
- Extended Detection & Response (XDR)
- Security Information and Event Management (SIEM)
- Network/device monitoring & response
- Managed detection & response (MDR)
- Network Detection Response (NDR)
- Security Operations Center (SOC) for around the clock (24/7/365) monitoring, detection, and response
- Logging practices/event logging
- Offsite/Immutable back-ups

The solution may be proposed as either a single product/offering or a combination of offerings that together offer the functionality that is required.

REMAINDER OF THIS PAGE IS LEFT INTENTIONALLY BLANK

4) Positive Identity Reinforcement

UTAW requires proposals in respect of updating its **Identity Protection and Authentication** stance and infrastructure. The proposal can be based either on the provisioning of a solution that will be owned and operated solely by UTAW (CapEx+OpEx Model), or as a subscription based offering whereby the combined costs of provisioning and maintaining the solution will be invoiced as recurring operational expenses ("OpEx") to UTAW. It can also be proposed as a hybrid of these two models.

The solution being proposed for this category must include the following functions:

- Cloud application protection
- Cloud Services
- Multi-Factor Authentication (MFA)/phishing-resistant MFA
- Identity governance & technologies
- Email and Web security

The solution may be proposed as either a single product/offering or a combination of offerings that together offer the functionality that is required.

5) Operational MDR

UTAW requires proposals in respect of enhancing its **Monitoring, Detection and Response** stance and infrastructure. The proposal can be based either on the provisioning of a solution that will be owned and operated solely by UTAW (CapEx+OpEx Model), or as a subscription based offering whereby the combined costs of provisioning and maintaining the solution will be invoiced as recurring operational expenses ("OpEx") to UTAW. It can also be proposed as a hybrid of these two models.

The solution being proposed for this category must include the following functions:

- Network Security Audit
- Network traffic analysis
- Managed Service Providers
- Penetration testing

The solution(s) may be provided as either a single product/offering or a combination of offerings that together offer the services that are required.

REMAINDER OF THIS PAGE IS LEFT INTENTIONALLY BLANK

Cybersecurity 85 Pilot Program Proposal Requirements

- 1.** The Cybersecurity Pilot Program is administered by the Schools and Libraries Division (SLD) of the Universal Service Administrative Co. (USAC) for the Federal Communications Commission (FCC). Discounts from the Cybersecurity Pilot Program will fund this Request for Proposal. Funding, if available, will be available as soon as a Pilot participant receives a Funding Commitment Decision Letter (FCDL) from USAC and has successfully completed Part 2 of the FCC Form 484 application.
- 2. Required Notice to Proceed.** UTAW will follow the purchasing policies of their governing board and requirements and procedures of the FCC's E-Rate program as administered by USAC to be eligible for all available funding. The implementation of any associated contracts resulting from this competitive bid process will be dependent on UTAW's issuance of a written Notice to Proceed. E-Rate funding notification alone will not signify Notice to Proceed.

UTAW reserves the right to deny any or all proposals associated with this RFP, even with USAC E-Rate funding approval. Furthermore, if beneficial to UTAW, it reserves the right to accept the pricing proposal and locally fund (proceed with project or purchase) regardless of E-Rate approval.

UTAW reserves the right to purchase some, all, or none of the products and services awarded under this contract for E-Rate FY2025 and subsequent E-Rate funding years covered by the agreement.

- 3. Cybersecurity Compliance.** Service providers (offerors) must comply with FCC Cybersecurity Pilot program rules as set forth by the Federal Communications Commission (FCC) and administered by the Universal Service Administrative Company (USAC).

Disqualification – FCC Form 498 ID Status. If the offeror is under FCC red light status or does not have an FCC Form 498 ID (service provider identification number), the offeror may be disqualified by the applicant. If at any time during the contract period the service provider is red lighted, debarred, or otherwise no longer eligible to participate in the Cybersecurity program, the applicant reserves the right to terminate the contract.

- 4. Equivalent products and services.** Proposals are requested should specify manufacturer, part, model number OR EQUIVALENT.
- 5. All Costs.** Pricing proposed by the bidder must include all costs. All costs to provide the product or service should be included in the pricing schedule. Price increases will not be allowed during the initial term quoted. Prices may be lowered based on market conditions.
- 6. Cost Allocation.** Bidders must clearly separate E-Rate eligible costs from ineligible costs.
- 7. Contracts.** Bidders for services other than tariff or month-to-month arrangements, must include a contract or legally binding agreement in response to this RFP with

signature block for both service provider and applicant. The agreement should be provided in form only and will not be completed and executed until after bids are awarded by UTAW and negotiations completed as applicable. Quotes are not considered a legally binding agreement.

UTAW will reserve the right to extend or abbreviate the contract period if such extension or abbreviation is necessary to make the Contract term coincide with an E- Rate "program year" or an extended service end date for an E-Rate program year pursuant to a "service delivery deadline extension" as those terms are defined by the Federal Communications Commission (FCC) and/or the Universal Service Administrative Company (USAC).

(see <https://docs.fcc.gov/public/attachments/FCC-24-63A1.pdf> for reference).

8. Proposals for Cybersecurity Pilot Program products and services.

- Proposals for equipment should clearly list the location where the equipment will be installed if that has been specified in the proposal. In the event that this is to be "on-premises" at UTAW, the location should be specified as "UTAW Main Data Center".
- Proposals should meet industry standards and comply with applicable local, state and federal codes and regulations. For example, network wiring/cabling should meet or exceed EIA/TIA standards and national Electrical code standards.
- If applicable, Equipment should be properly configured, installed and tested.
- Include all items necessary for equipment to be fully operational including necessary cabling, connectors, components, and if applicable, installation, configuration, travel, per diem, and any other applicable fees.
- All installed equipment and cabling should be labeled.
- In addition to standard labeling (i.e. patch panels labeled with cable number), equipment should be labeled with E-Rate information as follows:
 - ❖ Funding Request
 - ❖ Number (FRN) Form
 - ❖ 471 Application
 - ❖ Number Purchase
 - ❖ Order Number
 - ❖ Installation Date
- In the event that services are offered, Offerors must include a statement of work (SOW) in respect of such.
- Proposals for new equipment should include a standard manufacturer's warranty (up to three years)
- The value of any free products and/or services must be deducted from the cost of the proposal.
- Proposals may include installation and configuration proposals unless otherwise noted.

- Proposals should clearly describe all costs including (if applicable) installation, configuration, shipping and handling charges unless otherwise noted.

9. Site and Service Substitution (Contract Modification). UTAW hereby provides notice to all interested vendors that site and/or service substitutions may be necessary during the term of the contract. Any agreement signed as a result of this RFP should contemplate the possibility of UTAW changing products or services within the guidelines set forth by the FCC. All vendors are also hereby provided notice that UTAW may add new locations to its network during the life of the contract, and existing sites may move or close. The contract(s) entered into as a result of this RFP should allow for said site/service substitutions. Vendors are to describe their process for amending the contract to accommodate site/service substitutions during the contract term.

10. Request For Substitution

Bidder may, unless otherwise stated, offer any material, process, article, etc., which shall be materially equal or better in every respect to that so indicated or specified (Specified Item) and will completely accomplish the purpose of the Contract Document. The Service Substitution must be accompanied by evidence as to whether the proposed substitution:

- (1) Is equal in quality service ability to the Specified Item;
- (2) Will entail no changes in detail, construction and scheduling of related work;
- (3) Will be acceptable in consideration of the required design and artistic effect;
- (4) Will provide no cost disadvantage to UTAW;
- (5) Will require no excessive or more expensive maintenance, including adequacy and availability of replacement parts; and
- (6) Will require no change of the construction schedule

11. Cybersecurity Budget Requirements.

During the Cybersecurity application process and prior to issuance of Cybersecurity funding, the applicant may need to make changes to the quantities and items selected in order to stay within their cybersecurity pilot program budget approved by the FCC (see <https://docs.fcc.gov/public/attachments/DOC-408937A1.pdf>). The applicant may contact the awarded offeror to adjust quantities in order to meet the Cybersecurity budget allocated to UTAW. The selected service provider is expected to respond timely with revised proposals and contracts for the applicant to ensure that the selected products and services are at or below the applicant's budget cap. The selected service provider will need to provide all the information necessary regarding reduction in quantities and associated installation, configuration, shipping and handling charges.

12. Documentation and Audit Compliance.

- Service provider shall provide all warranty and product documentation related to products sold to UTAW.
- Service provider shall retain all documentation related to the purchase and payment, including Forms 474 and receipt of payment from USAC, for all

products and services provided to UTAW. Related documentation must be retained for a period of TEN years from the last date of service.

- If UTAW is audited by the Administrator of the program, the service provider shall fully cooperate with UTAW to provide any documentation related to the provision of discounted products and services as requested.

13. Invoicing

- The default method of invoicing for all Funding Requests (FRN) created as a result of this RFP will be the Form 474 Service Provider invoice (SPI) unless the applicant explicitly requests Form 472 Billed Entity Applicant Reimbursement method.
 - o The Service Provider agrees to bill and receive a portion of the payment for the provisions of goods and services described herein directly from USAC via the Form 474 Service Provider invoice (SPI). The maximum percentage the applicant will be liable for is the pre-discount amount minus the funded amount as shown on the FCC Funding Commitment Decision Letter (FCDL) and any identified ineligible costs. Upon the successful receipt or posting of a Funding Commitment Decision letter from the SLD and submission, certification and USAC approval of Form 486, the applicant shall pay only the discounted amount beginning with the billing cycle immediately following said approval.
 - o All Service Provider invoicing to USAC must be completed within 90 days from the last day of service in accordance with § 54.2001. Should the Service Provider fail to invoice USAC in a timely manner, the Applicant will only be responsible for paying its non-discounted share. Service Providers shall retain all documentation related to the purchase, payment, delivery and/or installation, including Forms 474 and receipt of payment from USAC, for all products and services provided to the applicant. Related documentation must be retained for a period of 10 years from the last date of service (see <https://docs.fcc.gov/public/attachments/FCC-24-63A1>).
- Within one (1) week of award, the awarded Service Provider will provide the Applicant with a bill of materials suitable for the Form 471 item 21 attachment. Approval for any deviation from the item 21 attachment must be obtained from the Applicant. Subsequent schedules of values and invoices for each site must match Item 21 attachment or subsequent service substitutions.

14. Service Provider Responsibilities

- The agreement herein is contingent upon the approval of funding from the Universal Service Fund's Schools and Library Program.
- The applicant requires that Service Providers make themselves thoroughly familiar with any rules or regulations regarding the FCC Cybersecurity Pilot program (see <https://docs.fcc.gov/public/attachments/FCC-24-63A1.pdf>)
- Service Providers are required to be in full compliance with all current requirements and future requirements issued by the SLD throughout the contractual period of any contract entered into as a result of this RFP.

- Service Providers are responsible for providing a valid Service Provider Identification Number (SPIN) at the time the RFP is submitted (see <https://www.usac.org/e-rate/service-providers/step-1-obtain-a-spin/>).
- Service Providers are responsible for providing a valid Federal Communications Commissions (FCC) Registration Number at the time the RFP is submitted (see <https://apps.fcc.gov/cores/publicHome.do>).
- Service Providers are responsible for providing evidence of FCC Green Light Status at the time the proposal is submitted. Any potential offeror found to be in Red Light Status must provide an explanation of the steps it is undertaking to be removed to Red Light Status and the expected timeframe for resolution. A Service Provider's sustained Red-Light Status may be grounds for contract termination as it could prohibit the Service Provider from providing E-Rate discounts in a timely manner which would cause harm to the Applicant (see <https://www.fcc.gov/general/red-light-frequently-asked-questions>).
- Products and services must be delivered before billing can commence. At no time shall the Service Provider invoice before October 1, 2025.
- Prices must be held firm for the duration of the associated Cybersecurity Funding Year(s) or until all work associated with the project is complete (including any contracts and USAC approved extensions)
- In the event of questions during a Cybersecurity pre-commitment review, post commitment review and/or audit inquiry, the awarded Service Provider is expected to reply within three (3) days to questions associated with its proposal.
- No change in the products and/or services specified in this document orders will be allowed without prior written approval from the Applicant and a USAC service substitution approval with the exception of a Global Service Substitution.
- The Service Provider acknowledges that all pricing and technology infrastructure information in its proposal shall be considered as public and non - confidential pursuant to 47 CFR §54.504 (2) (i) (ii)
- The Service Provider acknowledges that its offer is considered to be the lowest corresponding price pursuant to §54.511 (b). Should it not be the lowest corresponding price, the Service Provider must disclose the conditions leading to the applicant being charged more than the lowest corresponding price.
- This offer is in full compliance with USAC's Free Services Advisory. There are no free services that would predict an artificial discount and preclude the applicant from paying its proportionate non-discounted share of costs. The Service Provider agrees to provide substantiating documentation to support this assertion should the applicant, USAC, or the FCC request it. The service providers are prohibited from offering gifts or anything of value to Pilot participants (schools, libraries, or consortia). This includes free cybersecurity services or equipment offered outside of the competitive bidding process. Any free item or discounted service must be **clearly disclosed** in the procurement or invoicing process.
- The awarded Service Provider is required to send copies of all forms and invoices to the Applicant prior to invoicing USAC for pre - approval. Failure to comply with this requirement may result in the Applicant placing the vendor on an "Invoice Check" with the USAC.
- The contract must provide cancellation of services without financial penalties if a school is closed. Applicant may cancel services to a school without penalties after a 30-day notice to Service Provider.

- Goods and services provided shall be clearly designated as “Cybersecurity Eligible”. Noneligible goods and services shall be clearly called out as 100% non-eligible or shall be “cost allocated” to show the percentage of eligible costs per FCC/USAC guidelines.
- Any proposal submitted in response to this request must be compliant with the FCC’s Order (FCC 19-121) prohibiting the sale, provision, maintenance, modification, or other support of equipment or services provided or manufactured by Huawei, ZTE, or any other covered company posing a national security threat to the integrity of communications networks or the communications supply chain. See <https://www.fcc.gov/supplychain/coveredlist> By submitting a response, vendors are certifying compliance with FCC 19-121. In June of 2024, the Commerce Department added Kaspersky Lab prohibited companies on the Covered List (see https://www.usac.org/wp-content/uploads/erate/documents/cyber_pilot/webinar_slides/Service-Provider-Webinar_CBRFINAL.pdf).
- Within one (1) week of award, the awarded Service Provider must provide the Applicant with a bill of materials using the most currently available “Bulk Upload Template” located at <https://www.usac.org/erate/applicant-process/applying-for-discounts/fcc-form-471-filing/>. Subsequent schedules of values and invoices for must match the Bulk Upload Template or subsequent service substitutions.

OTHER TERMS:

Contract Term:

Bidder must clearly define contract terms for all pricing submitted. A contract entered into as a result of an award by UTAW under this Solicitation must be available to begin providing goods and/or services starting on October 1, 2025, and continue to be valid for a three-year term, expiring on September 30, 2028. “The applicant will reserve the right to extend or abbreviate the contract period if such extension or abbreviation is necessary to make the Contract term coincide with an E-Rate “program year” or an extended service end date for an E-Rate program year pursuant to a “service delivery deadline extension,” as those terms are defined by the Federal Communications Commission (FCC) and/or the Universal Service Administrative Company (USAC).”

Late Proposals: UTAW is not responsible for late proposals.

Proposal Cost:

UTAW will not be liable for any cost not listed in the bid response.

Ethics:

The proposer shall not offer gifts or anything of value nor enter into any business arrangement with any employee, official, or agent of UTAW.

Liability and Reserved Rights:

By submitting a bid, each bidder agrees to waive any claim it has against UTAW, and its respective employees arising out of in connection with the administration, evaluation, or recommendation of any bid; waiver of any requirements under the bid documents, or the contract documents, acceptance or rejection of any bids; and award of the contract.

UTAW reserves the right, at its sole discretion, to reject any and all bids, or any part thereof, that it receives as a result of this request for proposal. UTAW also reserves the right to

waive informalities, technicalities and minor irregularities in those bids received, and retains the right to negotiate separately with any source whatsoever, in any manner necessary, to serve the best interests of UTAW. UTAW will, at its discretion, award a contract to the most favorable responsible bidder(s) submitted in accordance with the requirements of the Bid Documents, submitting the best response that complies with the terms of this packet which UTAW believes is in the best interest of UTAW and best value to UTAW and which may not represent the lowest prices submitted.

By execution and submission of this bid, the bidder hereby represents and warrants to UTAW as follows: "The bidder has read and understands the bid documents and therefore made in accordance with those documents." The General Terms and Conditions are an integral part of this bid.

This bid must remain open for acceptance for a period of one month.

Please note that on any company contract that UTAW may be asked to sign, the venue shall be Kings County and the governing law shall be that of the State of New York. UTAW can only indemnify up to the amount allowed by law and we cannot agree to the use of arbitration in resolving conflicts.

This Bid does not obligate UTAW to award a contract or to pay costs incurred in the preparation or submittal of any offer. UTAW is not liable for any costs incurred by the vendor prior to the issuance of any agreements, contracts, or purchase orders, and will not pay for information solicited or obtained in response to this RFP. The information obtained will be utilized solely to determine the suitability of the products or services offered. Subsequent procurement, if any, will be in accordance with appropriate rules and regulations.

This document does not commit UTAW to pay any cost incurred in the preparation or submission of any proposal or to procure or contract for any services. UTAW reserves the right to amend this document by an addendum issued up to the date set for receipt of proposals. Changes to this bid, prior to opening, may be made in the form of an addendum. Addendums will be shared by UTAW's to any bidders that have submitted a bid by email. If revisions are of such a magnitude to warrant, in UTAW's opinion, the postponement of the date for receipt of proposals, an addendum will be issued announcing the new date.

Contract Changes:

No verbal agreement or conversation with any officer, agent or employee of UTAW either before or after the execution of the contract resulting from the document or follow-up negotiations shall affect or modify any of the terms or obligations contained in the written contract resulting from the RFP. No alterations to the terms and conditions of the contract shall be valid or binding unless made in writing and signed by the Purchasing Agent and an authorized contractor representative.

Use of UTA Documents:

No alteration to UTAW forms will be permitted, including substitutions, additions, deletions or interlineations, without written consent of UTAW. Reproduction of UTAW documents is permitted, so long as reproduced copies are exactly the same in size, format, and content as forms prepared by UTAW. Any proposal submitted in altered form shall result in rejection of such proposal at the option of UTAW.

Questions:

There are no other specifications other than what is included in this package besides what has been provided as attachments (if any) to this RFP. All questions and answers will be addressed by E-Mail. It is the vendors' responsibility to review the responses to ensure that they have received all addendums issued for this bid, as well as viewed all questions and answers that are referenced. Vendors finding errors, omissions, or corrections that need to be made to the specifications shall contact UTAW as soon as possible before the bid is due.

REMAINDER OF THIS PAGE IS LEFT INTENTIONALLY BLANK